Exploring Older Adult Susceptibility to Fraudulent Computer Pop-Up Interruptions

Phillip L. Morgan[1], Emma J. Williams[2], Nancy A. Zook [3], and Gary Christopher[3]

[1] School of Psychology, Cardiff University, 70 Park Place, Cardiff, CF10 3AT, United Kingdom (morganphil@cardiff.ac.uk)
[2] School of Experimental Psychology, University of Bristol, 12a Priory Road, Bristol, BS8 1TU, United Kingdom (emma.williams@bristol.ac.uk)
[3] University of the West of England – Bristol, Frenchay Campus, Coldharbour Lane, Bristol, BS16 1QY, United Kingdom {nancy.zook, gary.christopher}@uwe.ac.uk

Abstract. The proliferation of occasionally Internet connectivity and accessibility has been accompanied by an increase in cyber-threats, including fraudulent communications. Fake computer updates, which attempt to persuade people to download malicious software by mimicking trusted brands and/or instilling urgency, are one way in which fraudsters try to infiltrate systems. A recent study of young university students (*M* 18.52-years) found that when such pop-ups interrupt a demanding cognitive task, participants spent little time viewing them and were more likely to miss suspicious cues and accept these updates compared to when they were viewed without the pressure to resume a suspended task [1]. The aim of the current experiment was to test an older adult sample (N = 29, all >60 years) using the same paradigm. We predicted that they would be more susceptible to malevolent pop-ups [2]; trusting them more than younger adults (e.g., [3]), and would attempt to resume the interrupted task faster to limit forgetting of encoded items. Phase 1 involved serial recall memory trials interrupted by genuine, mimicked, and low authority pop-ups. During phase 2, participants rated messages with unlimited time and gave reasons for their decisions. It was found that more than 70% of mimicked and low authority pop-ups were accepted in Phase 1 vs ~80% genuine pop-ups (and these were all approximately 10% higher than [1]). This was likely due to a greater tendency to ignore or miss suspicious content when performing under pressure, despite spending *longer* with messages and reporting high awareness of scam techniques than younger adults. Older adult participants were more suspicious during Phase 2 performing comparably to the younger adults in [1]. Factors that may impact older adult decisions relating to fraudulent computer communications are discussed, as well as theoretical and practical implications.

Keywords: Cyber Security · Susceptibility · Older Adults · Task Interruption

1 Introduction

The number of older adults using computers and the Internet for communication and entertainment is increasing [4, 5]. Whilst the rapid proliferation of Internet connectivity and accessibility is associated with multiple benefits to both younger and older users, there have been alarming increases in cyber-threats across both population sectors. For example, a recent report highlighted that up to 45% of consumers have been the victim of cyber-crime [6]. Online fraud and scams are a growing problem across society, with the general public increasingly exposed to fake websites, emails and computer updates [7]. These communications attempt to persuade people to click on malicious links, unknowingly download malware or provide personal information, often by masquerading as established institutions or brands and creating urgent scenarios designed to instill a sense of panic in recipients [8,9]. In addition to the potential financial and psychological costs of becoming a victim of fraud [10], such fake communications have the potential to significantly disrupt consumer trust and engagement in online activities and e-commerce [11]. Understanding what makes people susceptible to responding to fraudulent communications is, therefore, vital in order to identify how susceptibility can be effectively reduced. This is not only key to inform behavior change interventions and interface design recommendations for those accessing the Internet for work purposes, but also for individuals, including older adults, who are increasingly using the Internet for purposes such as socializing, purchasing, and banking.

Older adults have traditionally been considered to be particularly at risk of fraud victimization [12]. This victimization has been linked with situational factors, such as greater social isolation [13]. However, research has suggested that cognitive mechanisms related to trust evaluations may also impact vulnerability, with older adults being more trusting of stimuli that contain cues which tend to provoke a higher degree of suspicion in younger adults; a finding reflected in differential neural activation [3]. Truth Default Theory [14] suggests that when evaluating communications, individuals default to considering communications to be trustworthy unless particular cues are identified that provoke suspicion. Thus, it is possible that in older adult populations, subtle suspicious cues within fraudulent communications may be less likely to trigger an evaluation away from the cognitive default of trusting information to be legitimate. Older adults have also been found to be more likely to report succumbing to Internet phishing scams than younger adults, with prior victimization not predicted by differences in executive functioning ability [2]. However, a recent study did not fully support these findings [15].

It could be that susceptibility to phishing is in part determined by the setting. For example, when reviewing a pop-up as a single task, older adults may accurately identify malicious intent. However, in a situation where a task is already in progress, being interrupted by a pop-up may in-crease susceptibly to scams as these situations would increase cognitive load and tap into executive functions, which have been found to decline with age [16]. Indeed, studies have found that older adults show higher global cost in terms of task switching, that they perform less well in tasks of di-vided attention, and that their selective attention is particularly negatively affected by interference in challenging situations [17, 18]. Older adults perform less well in tasks of divided attention [18], and their selective attention is worse when faced with

more challenging situations as they can be more proneness to interference effects [17]. Furthermore, older adults have also been shown to have greater difficulties in keeping track of multiple streams of information and this may manifest in prioritizing one stream and neglecting another [19, 20]. There is also evidence that older adults tend to focus on one task more and neglect the other [20]. Taken together, these findings would suggest that situations with a high cognitive load may lead to less advantageous decision making in older adults.

In their consideration of susceptibility to phishing emails within the general public, [21, 22] suggest that whether suspicious cues are noticed within fraudulent communications depends on the depth of processing that an individual engages in. Individuals who engage in more automatic, heuristic forms of processing are considered to be more vulnerable to the influence techniques used within these messages (e.g., urgency, compliance with authority, avoidance of loss) and neglect other, more suspicious, aspects of the communication, such as authenticity cues (e.g., accurate sender addresses). These are core parameters of the recently developed Suspicion, Cognition, Automaticity Model (SCAM: [22]). It is possible that any increased trust of such communications in older adults, therefore, may be due to a greater reliance on heuristic processing strategies that prioritize influence cues when making decisions. Although it should be noted that reliance on less cognitively demanding strategies amongst some older adults' may not always be negative, depending on the task, goal, and context; including time constraints [23].

A recent study by [1] considered these theoretically driven mechanisms in relation to judgements of fraudulent computer updates, using a task interruption paradigm to examine the effects of cognitive pressure on decision processes amongst university students (*M* age 18.56-years). They compared three message types differing in authority based upon the presence and/or accuracy of informational cues (e.g., spelling error, inaccurate website link, lacking a copyright symbol). Genuine authority messages were not affected by any of these issues, whereas mimicked authority messages contained all three cues to potential malevolence. Low authority messages, contained no sender details, no reference to the application that seemingly required updating, and no website link. When younger adults were interrupted by such messages, whereby their ability to engage in more considered, systematic processing of message content is reduced, they were more likely to miss suspicious elements, assuming that messages were genuine. This led to accepting almost as many mimicked as genuine authority messages and an alarming 56% of low authority messages. This might have been partly driven by the short amount of time participants took before making a response. This was approximately 5.5-seconds for both genuine and mimicked messages and only slightly higher for low authority messages (~6-seconds). As expected, serial recall memory was impaired in all conditions irrespective of message authority, although was markedly worse following low versus genuine authority messages. In a follow-up phase, where participants viewed messages in isolation under no time pressure, the percentage of low authority message accepts reduced to 27% and whilst there was an improvement for mimicked messages, 55% were still accepted.

The extent that the above findings apply to other population sectors, such as older adults, is currently unknown. For instance, are older adults more vulnerable to heuristic processes that scams rely on and therefore less likely to notice suspicious elements? Or, similar to younger adults, does this depend on the degree of cognitive

resource that individuals have available to process information at the time and/or the amount of time they allocate to make a decision when needing to return to a suspended task? These are issues that we attempt to address within the current study as understanding them is vital to ensure that effective mitigations and interventions can be developed that enable all consumers to safely engage with online activities.

The Current Study

The paradigm used by [1] is applied to an older adult population. Specifically, a task interruption paradigm is used, whereby participants complete a demanding serial recall task and are interrupted during this task by computer updates of varying legitimacy purporting to require urgent action. Participants must respond to these interruptions before they are able to continue with the serial recall task. Participants then respond to the same update messages during a questionnaire phase, where there are no additional cognitive demands. This allows for a comparison of response judgements when recipients are under differing degrees of cognitive pressure. As in [1], participants within the current study are also asked to elaborate reasons for their accept/decline decisions within the questionnaire phase.

Main Hypotheses

According to previous research, the presence of urgency and loss influence techniques within computer update messages, combined with the pressure of continuing with a suspended cognitively demanding primary task, should lead to participants failing to notice inconsistencies within messages and defaulting to a trusting stance [1, 14, 21, 22]. When individuals are under less cognitive pressure, however, these inconsistencies are more likely to be noticed and illegitimate messages declined. Thus the following hypotheses can be made:

If increased cognitive pressure makes older adults more susceptible to fraudulent messages due to a reliance on heuristic processing strategies, it is predicted that:

H1a) There will be no difference in response choice between genuine and mimicked or low authority messages during the serial recall task, due to a failure to identify inconsistencies in message content. Specifically, the proportion of 'message accepts' will be the same in the mimicked and low authority conditions as in the genuine authority condition.

H1b) Conversely, when participants have unlimited time to inspect the content of messages, mimicked and low authority messages will be declined significantly more than genuine messages, due to the identification of inconsistencies provoking suspicion regarding message legitimacy.

H1c) There will be no difference in serial recall performance between genuine and mimicked or low authority message interruption conditions, due to all messages being processed to an equal extent (i.e., heuristically) and therefore having an equal impact on primary task resumption. Though, and related to H1a, post-interruption serial recall performance *per se* will be higher than in [1] because older adult participants will spend less time viewing all message types than the younger adults in [1] in order to resume the interrupted task promptly to limit the degree of forgetting of previously encoded items.

2 Method

Participants. Twenty-nine participants from a Bristol UK-based group database of self-reported, community dwelling healthy older adults (over the age of 60) were recruited to participate in an experimental task advertised as a *multitasking* study. The experiment was one of a battery of studies (counterbalanced) conducted as part of the BRACE 2017-18 funded project: *Measuring executive functioning predictive of real world behaviors in older adults*. Sixty-one participants completed the entire battery, although nine were excluded due to Montreal Cognitive Assessment (MoCa: [24]) scores of less than 26. The mean age was 68.73-years (*SD* = 4.42); and approximately 2/3 of the sample were female. Exclusion criteria included a medical history of neurological or neuropsychiatric diagnosis or other medical issue (e.g., brain injury, substance abuse, visual/auditory deficits) that could impede or prevent the ability to complete the battery of tests.

Design. A repeated-measures design was adopted, whereby all participants completed the same computer task (phase 1) and post-task questionnaires (phase 2). Phase 1 included 27 serial recall memory (SRM) trials, with nine interrupted by pre-designed computer updates that required an 'accept' or 'decline' response. Messages were one of three types: genuine authority, mimicked authority, or low authority (see Fig 1 for examples), and there were three instances of each. Further details are provided below. Dependent variables included the number of to-be-remembered (TBR) items recalled in the correct serial order (Max. nine per trial) and the proportion of genuine, mimicked and low authority interrupting messages accepted (Max. three per condition).

Materials and Procedure. These largely followed [1]. Phase 1 involved participants completing 27 SRM trials whilst being periodically, although not continuously, interrupted by computer update pop-up messages. For each trial, participants were presented with a string of nine letters and numbers in the center of the screen for 9-seconds. This letter/number string then disappeared and following a 2-second retention interval was replaced with the words 'enter code' for 10-seonds. At this point participants were required to record as many numbers and letters that they could remember in the correct order. Each trial used a different number/letter string. Nine trials contained an interruption, consisting of system security-related update pop-up messages appearing in the center of the screen after the letter/number string had disappeared but before the instruction to start recalling the string. This message remained on the screen until the participant chose to either accept it by pressing corresponding keys on the keyboard. Only after participants had responded could they continue with the suspended SRM trial.

Computer update messages were the same as those used in [1], see Figure 1. This included three genuine authority update messages (i.e., contained specific details related to recognizable organizations or software manufacturers, such as accurate computer programme references, presence of a copyright symbol and genuine website links), three mimicked authority update messages (i.e., contained the same level of detail but included a spelling error, an inaccurate website link and lacked a copyright symbol) and three low authority update messages (i.e., contained no details relating to the sender of the communication, such as organization's or application's, and no web-

site link). All of these updates required an urgent response to counter a purported threat, and focused on e.g., anti-virus, program critical fixes, or expiry of licenses.

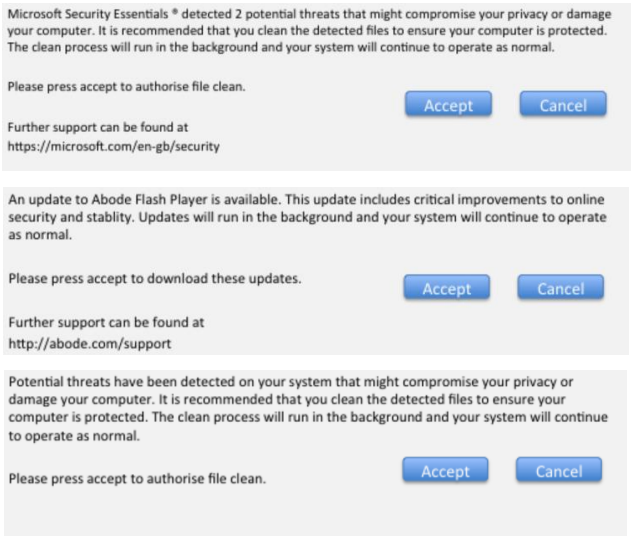

Fig. 1. Example genuine (top), mimicked (middle) and low (bottom) authority interrupting pop-up messages.

In phase 2, participants completed a computer-based questionnaire whereby they had unlimited time to re-evaluate each of the nine update messages and indicate whether they would ordinarily accept or decline them. Qualitative data was also collected by asking participants to explain each rating decision. Finally, participants were asked a series of 7-point Likert-scale questions related to cyber security awareness, which included: 'To what extent do you trust communications from your computer system, such as security updates, in general?'; 'How confident are you in your ability to differentiate genuine communications from scam communications in daily life?' and 'How would you rate your awareness of the common techniques used in scams?' In total, phase 2 took approximately 10 minutes. Participants were fully debriefed and given information on how to be more vigilant when dealing with online pop-up messages.

3 Results and Discussion

Scam Awareness, Trust, and Computer Usage

Participants reported a relatively high level of awareness of techniques used by scammers (M = 5.07; SD = 1.56; *Range* 1-7), although self-reported confidence to identify a scam (M = 4.21; SD = 1.82; *Range* 1-6) and trust in computer communications (M = 4.52; SD = 1.72; *Range* 1-7) were rated lower. Participants also reported spending on average 5.03-hours on computers a week and 4.28-hours per-week using the Internet.

Impact of Message Authority and Cognitive Complexity on Judgements

The number of messages accepted during phase 1 SRM trials and the questionnaire phase 2 are shown in Table 1 (and compared with [1]). A 2 (phase: serial recall, questionnaire) x 3 (message authority: genuine, mimicked, low) factorial repeated measures analysis of variance (ANOVA) revealed a significant main effect of phase, $F(1, 28) = 22.57$, $MSE = 1.55$, $p < .001$, with messages more likely to be accepted in phase 1 than 2. A significant main effect of message authority was also found, $F(2, 27) = 10.05$, $MSE = .335$, $p = .001$, as well as a significant interaction, $F(2, 27) = 9.01$, $MSE = .205$, $p = .001$. Bonferroni post-hoc comparisons revealed that during the SRM phase, participants were more likely to accept genuine than mimicked authority messages (*M Diff* = .31, $p = .005$, *CI* = .104, .516), in partial contrast to H1a. However, there were no significant differences in accept behavior across mimicked and low authority messages, or, low and genuine authority messages (all $ps > .2$), in line with H1a. Conversely, in the questionnaire phase, significant differences were found between all message types, with participants more likely to accept genuine messages than both mimicked (*M Diff* = .414, $p = .02$, *CI* = .069, .759) and low authority (*M Diff* = .759, $p < .001$, *CI* = .460, 1.058), and also mimicked than low authority messages (*M Diff* = .345, $p = .016$, *CI* = .071, .619), supporting H1b.

Table 1. Mean number of messages accepted per authority condition (Max. 3) when presented during the SRM and questionnaire phases. *Note.* Compared to findings of [1].

Message Authority	**Current Study Phase 1**		**Williams et al. (2017) Phase 1**		**Current Study Phase 2**		**Williams et al. (2017) Phase 2**	
	M	***SD***	***M***	***SD***	***M***	***SD***	***M***	***SD***
Low	2.34	.97	1.68	1.25	1.07	1.10	0.82	0.95
Mimicked	2.17	1.14	1.89	1.23	1.41	1.09	1.65	1.04
Genuine	2.48	.91	1.98	1.25	1.83	1.17	2.15	0.92

Impact of Pop-Up Message Interruptions Varying in Authority on Serial Recall Memory Performance

Serial recall memory performance was considered for all four conditions (no interruption, low authority interruption, mimicked authority interruption, and genuine authority interruption), see Figure 1. A repeated measures ANOVA revealed a significant main effect of interruption authority, $F(3,84) = 6.723$, $MSE = 1.03$, $p < .001$, with higher SRM performance in the no interruption condition compared to all interruption conditions ($ps < .02$). However, there were no significant differences in SRM performance between any of the pop-up message conditions (all $ps > .1$), supporting hypothesis H1c. This potential lack of processing differences between malevolent and genuine pop-up messages was further supported by findings of another repeated measures ANOVA, with a Huynh-Feldt correction applied due to violation of sphericity, which revealed no significant difference in participant response times (i.e., to select 'accept' or 'decline') across message type, $F(1.44, 40.32) = 4.09$, $MSE = 8.96$, $p = .60$: *M* GA response time = 10.45s; *M* MA response time = 10.92s; *M* LA response time = 11.00s. Interestingly, all mean response times were approximately 5 seconds longer than in the younger adult sample of [1], yet SRM performance post-

interruption was very comparable to that study (noting a marginally significant performance decline following low vs genuine authority interruptions in [1]).

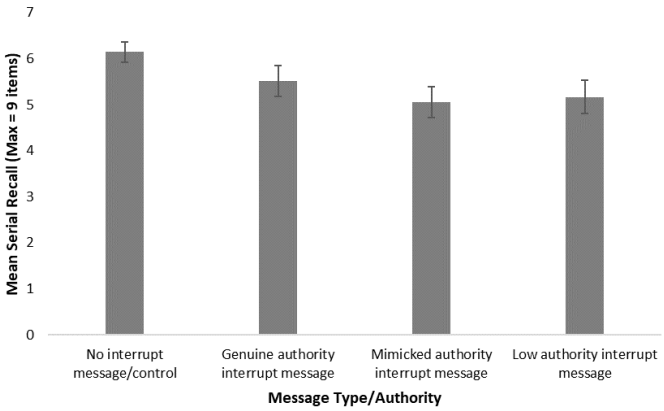

Fig 1. Effect of interrupt message type on serial recall memory. Note. Error bars represent ±standard error.

In combination, these findings suggest that when operating under a higher degree of cognitive pressure, older adult participants may have relied on more heuristic processing strategies linked to an inherent truth bias. However, participants did spend considerable time (relative to younger adults in [1]) with the messages onscreen before responding, which may have aided identification of inconsistencies for mimicked authority messages, and resulted in these messages being more likely to provoke suspicion [14, 22]. Conversely, low authority messages did not provoke suspicion when participants were operating under cognitive load, with such messages failing to contain overt information that could be used to trigger suspicion processes [14]. This failure to identify subtler triggers of suspicion during the serial recall task could be linked to previous suggestions of diminished 'gut responses' to suspicious cues in older adults [3], resulting in a continued default to considering the message to be legitimate.

When participants had more cognitive resource available (phase 2), however, they were better able to differentiate between fraudulent and genuine messages, with low authority messages considered to be the most suspicious (being accepted only 36% of the time) followed by mimicked authority messages (accepted 47% of the time). It should however be considered that participants were also more suspicious of genuine authority messages in this condition (accepted 61% of the time compared to 83% of the time in the serial recall condition), thus showing a reduced truth bias overall when more systematic processing of message content was encouraged.

Why Participants Chose to Accept or Decline Pop-Up Messages

Open-ended responses regarding why participants chose to accept or decline particular updates were analyzed using thematic analysis. The most common themes reported as impacting decision-making reflected those identified in the young adult sample of [1], and included:

• Reference to the *influence techniques* contained within the computer update messages, such as relating to known programs and/or respected organizations (e.g., "[] runs my computer programs so I trust them"), perceiving the action as urgent and important to undertake immediately ("Anything that mentions online security and stability immediately causes worry for me") or avoiding some form of security threat or other negative impact of some form of functionality (e.g., "important that the computer is protected")
• Reference to *potential authenticity cues*, such as spelling errors or inconsistencies, in raising suspicion (e.g., "Spelling mistake in [] suggests non-genuine source" and "No source quoted") or in appearing legitimate (e.g., "The link verifies that it can be verified as genuine"). Alternatively, this could relate to more subjective judgements, such as a communication either 'looking genuine' (e.g., "Source of message looks convincing" and "Seems genuine") or appearing to be 'not right' in some way (e.g., "Suspicious that this is a fake message and that accept will result in malware" and "Don't trust message"), with precise reasons for this not given.
• Reference to either *technical knowledge* (e.g., "I prefer my own security measures to []'s") or an *awareness of potential risks* of online fraud (e.g., "Anyone can call themselves []" and "It may not be what it claims; perhaps a scam"). This awareness was also reflected in the use of alternative verification strategies, whereby further verification or support would be sought if lacking technical knowledge (e.g., "Would check with the university IT Dept", "Unsure, so would ask husband", "I would have confirmed beforehand after getting support from the link" and "ask expert").
• Reference to *routine behaviors*, such as always declining certain types of update (e.g., "Wouldn't accept anything as their security software screens everything" and "I would never accept a clean process from a pop-up").

4 Limitations

There are a number of limitations to the current study that warrant noting and future attention. First, the sample size (N = 29) was much lower than in [1] (N = 87). Whilst this would normally be respectable given the independent variables tested and withstanding adequate power to detect medium to large effect sizes (f = .25-.4, [25]), there might possibly be greater cognitive ability differences within the older adult sample in relation to processes such as short-term memory and attention-inhibition. These factors have been measured as part of the larger study although have not yet been analyzed in relation to the current findings. For example, it could be the case that older adults with a higher verbal working memory span would feel less pressured to resume the primary task faster (and also respond to a pop-up message faster) than individuals with a lower span. Second, we noted early on that typically fewer (~41-78%) participants in our tested age range reported regularly using the Internet compared to the ~99% of younger adults identified in previous work [5]. Thus older adults might be less familiar with Internet pop-ups than younger adults. This may have impacted the findings and in future should be considered as a possible co-variate. Third, and related to the last point, it may be the case that a greater number of older adults are less familiar with the brand and company names used within genuine and mimicked messages (e.g. Adobe Flash Player, AVG Internet Security, Microsoft Visual Basic). Whilst this

does not seem to be able to account for the differences between accept rates for genuine versus mimicked authority messages (i.e., should be similar if brand/company familiarity was an issue), familiarity is a factor that should be controlled for in future studies. Fourth, participants were not using personal computers and instead used university computers under controlled laboratory conditions. This could mean that the perceived consequences of accepting more messages, despite their authority, was not deemed critical to the participants (i.e., 'what is the worst that can happen?'). Additionally, many may have perceived the university laboratory to be a safe and secure environment and felt that the computers would be protected against possible cyber threats and/or equipped to deal with any that get through. Either way, this means that the findings need to be treated with a degree of caution in terms of possible generalizability to personal computer usage situations. Fifth, our sample were predominantly high functioning and mostly well educated, and so perhaps atypical of a less self-selecting sample. This could have been linked with them being more aware of online safety issues. Finally, whilst we can assume that older adult participants were engaging in greater visual and possibly heuristic processing of pop-up messages during the 10-11-seconds taken to make a response compared with the younger participants in [1] (who responded ~5-seconds faster), both studies are lacking eye movement, fixation, and pupilometry (e.g., pupil size variations) data. This is a factor that requires attention in future studies if firm conclusions are to be made about what participants are processing, when, for how long, and to what depth.

5 Implications

There are a number of implications of the current study findings that warrant future attention. A key and alarming finding is that despite our older adult sample accepting fewer mimicked than genuine authority messages under conditions of high cognitive (specifically memory) load, 72% of all mimicked authority messages were accepted when 100% should have been declined if cues to potential deception were detected and acted upon. Worse still, 78% of low authority messages (containing no sender details, application details, website links or other cues to authenticity, such as copyright symbols) were accepted. Like younger adults [1], albeit to a greater extent, older adults seem to demonstrate a very high degree of susceptibility to potentially malevolent online pop-up messages masquerading as innocent and important computer update messages. Thus, at least two implications follow. First, older (and younger) adults seem to require better training into techniques and strategies for determining the legitimacy of computer-based communications such as pop-up alerts. Such interventions could involve training to detect cues to potential malevolence and allowing a sufficient amount of practice delegated to learn the procedure(s).

However, the scenarios we have tested involve responding to pop-up messages whilst a high cognitive load memory based task has been suspended. So benefits of such training may be minimal if people are determined to deal with pop-ups promptly and return to the primary task. One idea is to train individuals to decline pop-up type messages when they occur under such cognitively taxing circumstances to minimize the risk of making a costly mistake. However, this will not always be possible (e.g., in safety- and/or time- critical situations) and may result in compromising the smooth

and efficient running of the computer and its applications. Therefore, and second, we advocate the development of interface design features that on one hand should support users to dedicate more cognitive effort to checking the integrity of update type messages (e.g., offer informative feedback, permit easy reversal of actions: e.g., [26]) whilst not compromising the performance of a primary task (e.g., include flexible time periods to re-inspect and respond to messages, user control and freedom with clearly marked exits such as a 'not now' option: e.g., [27]). In the case of older adults, there are a range of relevant interface design principles (e.g., [28, 29, 30]), including: avoid complex or long messages to avoid memory/information overload; clearly label items (especially those that are complex); use simple, minimal and intuitive steps in order to perform tasks; and, avoid using time pressure (e.g., perform x in 10-seconds, choose 'yes' or 'no'). Each of these and numerous other interface design recommendations, together with better training into techniques and strategies for determining the legitimacy of computer-based communications need careful consideration in the future to minimize susceptibility to potentially malevolent online threats amongst both younger and perhaps more crucially older adult Internet user populations.

Acknowledgments. The reported research forms part of a United Kingdom BRACE funded project (2016-17) – Measuring executive functioning predictive of real world behaviours in older adults. We thank a number of people for assistance with data collection including: Emma Gaskin, Kiren Bains, Laura Bishop, Michael Carmody-Baker, Zahra Dahnoun, Ellie MacFarlane, Katerina Stankova, and Rose Vincent.

References

1. Williams, E.J., Morgan, P. L., Joinson, A.J.: Press accept to update now: Individual differences in susceptibility to malevolent interruptions. Decision Support Systems, **96**, 119-129 (2017)
2. Roberts, J., John, S., Bussell, C., Grajzel, K., Zhao, R., Karas, S., Six, D., Yue, C., Gavett, B.: Age group, not executive functioning, predicts past susceptibility to Internet phishing scams, Archives of Clinical Neuropsychology, **30**(6), 572-573 (2015)
3. Castle, E., Eisenberger, N.I., Seeman, T.E., Moons, W.G., Boggero, I.A., Grinblatt, M.S., Taylor, S.E.: Neural and behavioral bases of age differences in perceptions of trust, Proceedings of the National Academy of Sciences USA, **109**(51), 20848-29852 (2012)
4. Gatto, S.L., Tak, S.H.: Computer, Internet, and email use among older adults: Benefits and barriers, Educational Gerontology, **34**(9), 800-811 (2008)
5. Office for National Statistics.: Internet users in the UK: 2017. Available from: https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2017 (2017)
6. Infosecurity Magazine.: 45% of consumers are victims of cybercrime. Available from: https://www.infosecurity-magazine.com/news/45-of-consumers-are-victims-of/ (2016)
7. McAfee.: What is Fake Antivirus Software? Available from: https://securingtomorrow.mcafee.com/consumer/family-safety/fake-antivirus-software/ (2014)
8. Atkins, B., Huang, W.: A study of social engineering in online frauds. Open Journal of Social Sciences, **1**(3), 23-23 (2013)

9. Workman, M.: Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the American Society for Information Science and Technology, **59**(4), 662–674 (2008)
10. Deem, D.L.: Notes from the field: Observations in working with the forgotten victims of personal financial crimes. Journal of Elder Abuse & Neglect, **12**(2), 33-48 (2000)
11. Smith, A.D.: Cybercriminal impacts on online business and consumer confidence. Online Information Review, **28**(3), 224-234 (2004)
12. James, B.D., Boyle, P.A., Bennett, D.A.: Correlates of susceptibility to scams in older adults without dementia. Journal of Elder Adult Abuse and Neglect, **26**(2), 107-122 (2014)
13. Lichtenberg, P.A., Stickney, L., Paulson, D.: Is psychological vulnerability related to the experience of fraud in older adults? Clinical Gerontology, **36**(2), 132-146 (2013)
14. Levine, T. R.: Truth-default theory: A theory of human deception and deception detection. Journal of Language and Social Psychology, **33**, 378-392 (2014)
15. Gavett, B.E., Zhao, R., John, S.E., Bussell, C.A., Roberts, J.R., Yue, C.: Phishing suspiciousness in older and younger adults: The role of executive functioning. PLOS One, 0171620 (2017)
16. Bruine de Bruin, W., Parker, A.M., Fischhoff, B.: Explaining adult age differences in decision making competence, Journal of Behavioral Decision Making, **24**, 1-14 (2010)
17. Bäckman, L., Molander, B.: Adult age differences in the ability to cope with situations of high arousal in a precision sport, Psychology and Aging, **1**(2), 133 (1986)
18. Verhaeghen, P., Cerella, J.: Aging, executive control, and attention: A review of meta-analyses, Neuroscience & Biobehavioral Reviews, **26**(7), 849-857 (2002)
19. Charness, N.: Aging and problem-solving performance, In N. Charness (Ed.), Aging and Human Performance. Wiley, New York, 225-259 (1985)
20. McDowd, J. M., Vercruyssen, M., Birren, J. E.: Aging, divided attention, and dual-task performance. Multiple-task performance, 387-414 (1991)
21. Vishwanath, A., Herath, T., Chen, R., Wang, J., Rao, H. R.: Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, **51**, 576-586 (2011)
22. Vishwanath, A., Harrison, B., Ng, Y. J.: Suspicion, cognition, and automaticity model of phishing susceptibility. Communication Research, online pre-print, 1-21 (2016)
23. Mata, R., Schooler, L. J., Rieskamp, J.: The aging decision maker: cognitive aging and the adaptive selection of decision strategies, Psychology and Aging, **22**(4), 796 (2007)
24. Nasreddine, Z. S., Phillips, N. A., Bedirian, V., Charbonneau, S., Whitehead, V., Collin, I., Cummings, J. L., Chertkow, H.: The Montreal Cognitive Assessment, MoCA: a brief screening tool for mild cognitive impairment, Journal of the American Geriatric Society, **53**(4), 695-699 (2005)
25. Cohen, J.: Statistical power analysis for the behavioural sciences. Lawrence Earlbaum Associates, Hillside, NJ (1988)
26. Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., Elmqvist, N.: Designing the User Interface: Strategies for Effective Human-Computer Interaction: Sixth Edition, Pearson (2016)
27. Nielsen, J.: Heuristic evaluation. In Nielsen, J., and Mack, R.L. (Eds.), Usability Inspection Methods. John Wiley & Sons, New York (1994)
28. Farage, M. A., Miller, K. W., Ajayi, F., Hutchins, D.: Design principles to accommodate older adults, Global Journal of Health Science, **4**(2), 2 (2012)
29. Sharit, J., Czaja, S. J., Nair, S., Lee, C. C.: Effects of age, speech rate, and environmental support in using telephone voice menu systems, Human Factors, **45**(2), 234-251 (2003)

30. Zaphiris, P., Kurniawan, S., Ghiawadwala, M.: A systematic approach to the development of research-based web design guidelines for older people, Universal Access in the Information Society, **6**(1), 59-75 (2007)